SECURE PORTING OF INFORMATION FROM ONE DEVICE TO ANOTHER

Field of the Invention

[0001] This invention relates to schemes for securely porting information between devices, and more particularly to preventing unauthorized transfer of such information.

Background of the Invention

[0002] It is often desirable or convenient to transport audio or video information from one device to another. For example, music stored on a home device may be copied to a medium for playing in an automobile. In the past, such a transfer of music might be accomplished by recording from an analog vinyl disk onto an audio cassette which could be played in the automobile. The owners of the copyrights in the music material could be reasonably sure that the music could not be usefully replicated to many generations, because inexact analog reproduction and the multiplication of noise would degrade the quality of the performance after a few generations.

[0003] With the advent of digital recording and storage, the potential exists for the making of many generations of essentially perfect copies of information, be it audio or video. Various schemes have been suggested and implemented in attempts to limit the unauthorized copying of digitally recorded entertainment media.

[0004] Improved and/or alternative arrangements are desired for secure porting of digital information.

Summary of the Invention

[0005] A method according to an aspect of the invention is for securely porting or transferring digital information from a source of digital information to a destination device. The source device includes a removable digital memory including a port at which the digital information can be accessed. The source device also includes a stored first Conditional Access Certificate and also includes an access card port or slot. A destination device includes a digital information port which is capable of receiving the digital information, and further

includes an access card port or slot. The destination device further includes a stored second User Certificate, and also includes mutually corresponding private and public encryption keys associated with the destination device. An access card is provided, which is capable of use with both the source device and the destination device. The access card includes a second Conditional Access Certificate and a first User Certificate stored therein. After the placing of the access card in the access card port of the destination device a first time, the User certificate in the destination device is accessed by the access card, and, within the access card, the second User Certificate from the destination device is authenticated using the second Conditional Access Certificate from the access card, to determine if the public encryption key from the destination device should be written to the access card. In a preferred embodiment, the public encryption key is not written to the access card if the access card already contains a public key from any destination device. If it is determined that the public encryption key of the destination device should be written to the access card, the public encryption key from the destination device is written to the access card. The access card is removed from the destination device after the writing of the public encryption key. The access card is then inserted into the access card port of the source device. At least the first Conditional Access Certificate stored in the source device is used to determine if the first User Certificate stored in the access card is valid. If the access card is deemed to be valid by the source device, the public encryption key is copied from the access card to the source device. At the source device, at least some of the digital information in the digital memory is encrypted using at least one content encryption key to produce encrypted information. At least one content encryption key is encrypted using the public key portion of the public/private encoding key pair from the destination device. The least one encrypted content encryption key is stored in the access card. The port of the digital memory is connected to the digital information port of the destination device. The access card is placed in the access card port of the destination device a second time. Then the

encrypted content encryption key is copied from the access card to the destination device, and decrypted using the destination device's private key. The encrypted information from the digital memory is received at the destination device, and decrypted using the decrypted content encryption key.

[0006] In a particularly advantageous embodiment, the Conditional Access certificate is evaluated to determine if it is expired. One embodiment compares the current time with a time stamp found within the Conditional Access certificate.

Brief Description of the Drawing

[0007] FIGURE 1 is a simplified diagram illustrating a digital information source device with removable memory, and a data destination device, together with an access card, all as purchased from a vendor;

FIGURE 2 illustrates the elements of FIGURE 1, with the access card plugged into the destination device for authenticating the destination device and for receiving a public key portion of an encryption key;

FIGURE 3 illustrates the elements of FIGURE 1 after the state illustrated in FIGURE 2, with the access card plugged into the source device for authenticating the access card by use of a conditional access certificate in the source device, and for loading of the public key portion of the encryption key into the source device;

FIGURE 4 illustrates the elements of FIGURE 1 after the state illustrated in FIGURE 3, with the source device encrypting the content of the removable memory, and storing the encrypted content encryption key in the access card;

FIGURE 5 illustrates the elements of FIGURE 1 after the state of FIGURE 4, showing the access card again plugged into the destination device for transfer of the encryption key to the destination device, and also showing the memory plugged into the destination device for transfer of the encrypted information to the destination device for decryption by the destination device.

Description of the Invention

[0008] FIGURE 1 illustrates the individual source device 12, destination device 30, and access card 40 in their as-purchased state. The devices 12 and 30, and the card 40, may be purchased at different times and different locations. As illustrated in FIGURE 1, source device 12 includes a device 14 and an associated removable mass memory device 18, designated a hard disk drive (HDD) in this example. The memory 18 is connected to the device 14 by way of a data path 20, which is preferably a high-speed data path such as USB 2.0. Device 14 may be viewed as being a housing with a processor, which accommodates and powers removable memory 18, and provides it with external ports and signals. Such a device might be similar to a Personal Video Recorder such as might be associated with a digital television settop digital receiver, but with the added feature of having the memory removable and transportable independently of the device 14.

[0009] As illustrated in FIGURE 1, device 14 also includes a card slot 22 and a physically secure memory 16, such as a ROM, preloaded by the vendor with a Conditional Access (CA) Certificate designated as A.

[0010] The source device 12 of FIGURE 1 can be used by the owner to record audio or video media for reproduction by device 12 for the user's purposes. At some later time, or possibly concurrently with the purchase of the source device 12 of FIGURE 1, the owner (or lessee, as the case may be) of source device 12 may acquire or lease a device capable of being loaded with digital media for use at a location remote from source device 12. Such a device might be, for example, a car player for digital audio or video, and it is denominated as destination device 30 in FIGURE 1. Destination device 30 includes a card slot 38, and also includes an internal memory 32 which is preloaded with a User Certificate designated as A. Another memory set, designated 34 and 36, within destination device 30 is preloaded with the private and public key portions, respectively, of a key encryption key pair. While not absolutely necessary, it is desirable that the destination device 30 also contain a unique string of characters which allow it to be uniquely identifiable as a non-volatile memory

location. Such a unique string might include codes identifying the make, model, and possibly the VIN of the car in which the destination device is located. Finally, destination device 30 includes a data port 30_{data}, which may be a USB 2.0 port. Thus, both the device 14 and the destination device 30 act as independent USB 2.0 hosts in this embodiment.

[0011] The owner of the source device 12 and the destination device 30 of FIGURE 1 may desire to play the audio or video media stored in memory 18 on his destination device 30. If the digital audio, video or other data content were left unencrypted on the memory 18, an unscrupulous owner could copy the data endlessly and use the data on unauthorized devices. The source device should not store any unencrypted data on memory device 18 which has any value to pirates. According to an aspect of the invention, the user wishing to transfer information from source device 12 to destination device 30 acquires or purchases an access card 40, illustrated in FIGURE 1 as including a memory set 42, 44 preloaded with a conditional access (CA) certificate designated A and a User Certificate designated B. While not essential to the invention, the access card as purchased may include a timing function or time identification which allows the card to be used only for a particular period of time. If the time has expired, the source device may prompt the user to purchase a new card.

[0012] According to an aspect of the invention, the destination device 30 is identified to the access card by inserting the access card into the slot 38 of the destination device, as illustrated in FIGURE 2. A first (1) processing step, illustrated by line 210 in FIGURE 2, is to authenticate the destination device by processing the User Certificate A stored in memory 32 of the destination device with the CA Certificate A stored in memory 42 of the access card. As an example, a company will produce or have produced unique company specific Conditional Access certificates, which may be "A" or "B" and also produces physical devices. The physical devices may be as simple as a personal computer with software suited to the method of the invention. The physical devices produce two series of certificates in the form of streams of data of User

Certificates on demand. One stream can be validated using Conditional Access Certificate A and the other stream can be authenticated using Conditional Access Certificate B. These User Certificates may each be unique, but have in common the characteristic that, once entered into an authenticating algorithm together with the Conditional Access Certificate, will produce an "authenticated" result, as known in the art. Each of the source, destination, and access card is loaded with User and Conditional Access certificates during manufacture. In one possible use, an "RCA" or "Thomson" access card could be purchased from a retail vendor of electronics equipment.

[0013] If the authentication is properly completed, the access card 40 reads the public key portion of the encryption key, stored in memory 36, into a conventional write-once, nonvolatile memory 46 located in the access card 40, as suggested by line 212 of FIGURE 2, together or paired with the unique identification string. This step may be considered to be a second processing step (2). The access card is now loaded with information relating to the device for which the data stored in memory 18 is destined, meaning that it has a one-to-one correspondence (i.e., paired) with the destination device. This process of first insertion of the access card need only be performed once to establish the one-to-one correspondence between the destination device and the access card. At the completion of the authentication and loading of the access card associated with the first insertion, the destination device (or even the access card) may give a signal that the process is complete, as by illuminating a light emitting diode (LED) or by other signal.

[0014] Following the step illustrated in FIGURE 2, the access card is removed from slot 38 of destination device 30, and is transported to, and inserted into, slot 22 of source device 12, as suggested in FIGURE 3. According to an aspect of the invention, the User Certificate B stored in memory 44 of access card 40 is read by the source device 12 and processed together with CA certificate B stored in memory 16 of device 14, to authenticate the card 40. This may be considered to be a third (3) processing step, and is illustrated in FIGURE 3 by line 310. The authentication step 310 must be performed in

device 14. The authentication may include verification that the time limit of the access card is not expired. Following the authentication of the card, the public key encryption key stored in memory 46 of access card 40 is transferred to a memory portion 318 of device 14.

[0015] Following the transfer of the public key portion of the encryption key to memory portion 318, device 14 of FIGURE 4 encrypts the data to be stored in memory 18 using its own encryption keys, and loads or returns the encrypted data, illustrated as 418, to the memory 18. This may be viewed as being a fifth (5) processing step, illustrated by a solid line 405 in FIGURE 4. It should be noted that different content encoding keys may be used for different portions of the data to be transferred, such as a first content encoding key for the audio, a second for the video, and a third for other data. Alternatively, the content to be transferred may be broken into separate portions, if desired, each encoded with a different content encoding key. The locally generated encryption key(s) is/are at least temporarily stored in a memory portion 414 for the duration of the encryption of the data. The device 14 also encrypts its own content encryption key(s) using the public encryption key stored in memory portion 318, and the content encryption keys so encrypted are written to a memory portion 440 of access card 40 of FIGURE 4 as a sixth (6) step, illustrated as a solid line 406. Once the public-key encrypted content encryption keys are transferred to access card 40, the public key (originating from the destination device and transferred via the access card) may be erased from memory portion 318, so that it is later available for use to store the public key of some other destination device, derived from another, different access card.

[0016] Following the storage in memory 18 of the encrypted data to be transferred to the destination device 30, the memory is moved to the location of the destination device 30, and its data path 20 is connected to data port $\mathbf{30}_{data,}$ as illustrated in FIGURE 5. The access card is removed from card slot 22 of the device 14, and is moved to destination device 30, and plugged into its card slot 38. This represents a second insertion of the access card 40 into the destination device 30. The

encrypted content encryption keys stored in memory 440 of access card 40 are transferred to a memory portion 540 of destination device 30. Destination device 30 uses its private key to decrypt the content encoding key(s) for use in decrypting the encrypted data from memory 18 for playback, display or use.

[0017] In operation of the method, the removable access card 40 stores authorization and decryption data which are to be transported from one physical device to another. Information relating to the destination device 30 is stored on the access card 12 which, acting as a proxy, authenticates the destination device 30 to the source device 12. The source device 12, after authenticating that the destination device 30 is from a valid or authorized vendor, can store encrypted content encryption keys on the access card 40 for use by the destination device 30. The destination device can then decrypt the encrypted keys to obtain keys for decryption of the encrypted audio, video or other digital data stored on the separate memory or hard drive.

[0018] The access card should authenticate the destination device at first insertion, because an invalid destination device, if it were to be loaded with the content of memory 18, could be used for improper purposes, such as for the making of unauthorized copies. The access card should be authenticated by the source device, to protect against rogue access cards which may have bypassed the authentication of the destination device.

[0019] If one were to attempt to use the access card to load some destination device (i.e., a rogue destination device) other than destination device 30 with which the access card is paired, that rogue device would not be able to decrypt the content encryption keys, because its public/private key ensemble is different from that of destination device 30. Thus, after the first insertion, there is a one-to-one pairing between the access card and the associated destination device. Since at least memory portion 46 of the access card 40 is write-once, the card cannot be re-used by inserting it "a first time" into another destination device and overwriting that memory portion. Either the card or the second destination

device with which an attempt is made to use the card may advise the user that the card is already paired with the XYZ Video player in your ABC sedan, and cannot be used with the second destination device. This, in turn, requires that the customer purchase another access card in order to load the further destination device.

[0020] Because the public key is not distributed with the access card, but is instead written to the access card by the selected destination device at its first insertion, there is not a one-to-one correspondence between an unused or unpaired access card and any destination device. The unused access cards are therefore generic and can be paired with any destination device by the first insertion process. Thus, the access cards can be manufactured without special or individual content. The lack of advanced knowledge of the identity of the destination device reduces the manufacturing cost and the complexity of the distribution process. Avoidance of a pre-sale pairing between access cards and destination devices greatly simplifies the post sale accessory purchase of an access card by a destination device owner. When he later returns to the store to purchase an access card, no one specific card is needed for his device, as any unused card will work.

[0021] If an unused or unpaired access card is inserted into the source device, the source device will detect the lack of both a public encryption key and the identification string of a destination device. In this case the source device can provide a message such as "This Access Card must first be inserted into the destination player you plan to load."

[0022] The arrangement according to the invention prevents an owner of a source device such as 12 of the *FIGURES* from using the same card with two or more destination devices such as 30, because the individual destination devices have different encryption codes stored therein, and thus a separate card must be used for each transfer. Only one destination device has the private key which can decrypt the encrypted content encryption keys stored on the digital memory device or card. This is the destination device with which the access card was originally paired during the first insertion operation. Other or rogue destination devices can read the

encrypted data and also read the encrypted content encryption keys, but cannot decrypt the encrypted content encryption keys to obtain the content encryption key, and therefore cannot decrypt the encrypted data.

[0023] The authentication information on the access card may be set to expire at a given time or after a given interval after first use, thereby requiring customer renewal.

[0024] In a particularly advantageous embodiment, the User Certificate of the Access Card is evaluated by the Source Device to determine if it is expired. One embodiment compares the current time with a time stamp found within the User Certificate.

[0025] Although the invention has been described in terms of exemplary embodiments, it is not limited thereto. The appended claims should be construed broadly to include other variants and embodiments of the invention which may be made by those skilled in the art without departing from the scope and range of equivalents of the invention.